**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

**Security Equipment**

**Security Hardware**

1. **What is meant by data integrity?**

Data integrity is the assurance that data is accurate and reliable, and is available in a timely manner.

1. **Biometrics**
   1. **Describe biometric security.**

Biometric security is theuse of physical human characteristics, including finger prints of facial features, or behaviour characterises as such as voice patterns, or handwriting, to authenticate a user before granting them access to data.

* 1. **Why does it appeal to security managers?**

It appeals to managers because it is almost impossible to copy or steal a person’s biometric characteristics.

* 1. **List the common biometric devices.**
* Voice recognition
* Finger prints
* Hand geometry
* Signature recognition
* Facial recognition
* Iris recognition
  1. **What are the concerns of biometric technology?**

The hardware can be seen as intrusive, especially iris scanning.

1. **Swipe cards**
   1. **Describe the nature of a swipe card.**

A swipe card is a plastic, business sized card with a magnetic strip on one side.

* 1. **What is a limitation of the swipe card?**

Swipe cards are easily stolen and damaged.

1. **Smart cards**

Smart cards are much the same as swipe cards except for that they contain a microchip that can store and manipulate data. Some common examples are the myki public transport system and prepaid telephone cards.

1. **Security tokens**

Security tokens are used when sensitive information. They are the size of a key ring and they are used to display and authentication code. When the user wishes to access the information they need to enter in their username and password and then the authentication code displayed on the security token. This code will change every 5 mins and it will provide an extra level of assurance known as two factor authentication, because the two sets of information are needed. This type of security is widely used by financial institutions for online banking.

1. **Mobile phone secure code**
   1. **How does this level of authentication work?**

This is another type of security that is used by financial institutions and it uses a mobile phone to operate. When the user wants to transfer money to other accounts, a code is sent to the mobile of the customer to authenticate the transaction before it occurs. The account holder then needs to log on and enter the code before the transaction can occur.

**Power protection**

**Outline the characteristics of the following:**

1. **Surge protector**

A surge protector will protect electrical equipment against overvoltage by smoothing out the currents coming from the main supply. It will also block sudden surges, also known as spikes. The surge protector may be damaged by a spike but it will prevent the current from reaching the equipment.

1. **Uninterruptible power supply, (UPS)**

Uninterruptible power supply (UPS) will also protect against spikes and also help to protect data if there is an undercurrent or a complete power failure. When a loss of electricity occurs the UPS’s batteries will kick in and allow 10-30 minutes of power, so that the owner can back up data or shut down the equipment properly.

**Strategies for avoiding system failure, p 288**

1. **What is meant by redundancy?**

Redundancy means that no part of the system is crucial to its overall operation.

1. **What is meant be a fault-tolerant server?**

A fault tolerant server will continue to work even when a piece of hardware has failed. This is achieved by having multiple components, such as multiple hard disks or motherboards.

1. **Redundancy through multiple hard drives or fault-tolerant equipment**
   1. **Describe how this redundancy works.**

This works through allowing the system to still run as normal because of the multiple hard disks, while a technician repair the faulty hardware.

* 1. **What is meant by RAID technology**

RAID stands for random display of inexpensive disks. It means that the data is stored on more than one disk so that if one fails, not all the data is lost.

1. **Redundancy through mirrored servers or machines**
   1. **Why is the RAID solution preferable to this solution?**

It is common to copy data onto a second hard drive so that there are two hard disks with all of the data on them. This means that there are two sets of data available in case on fails.

**Backup Media**

1. **There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?**

* Speed
* Cost
* Compatibility

**Three categories of backup media:**

**List the characteristics of the following backup media:**

**Magnetic media**

1. **Hard Disk Drive**

* Affordable
* Useful for many files
* Usually offsite

1. **Magnetic Tapes**

* Popular
* Cheap
* Slow in saving and restoring files
* Sequential
* Many organisations have automatic tape backup

**Optical media**

1. **Compact disc**

* Hold up to 700MB of data (80mis of audio)
* CD-Read = Only write data once
* CD-RW = Write data a number of times

1. **DVD**

* This backup media has recently grown in popularity
* Stands for digital versatile disk or digital video disk
* They can be used once or many times

1. **Blu-ray**

* Relatively new
* Capacity of 50GB
* Dual layer
* The name blu-ray originates from the blue laser used to read the disk
* Allows HD films to be stored

**Solid-state drives**

1. **USB storage devices**

* Popular
* Small
* Conveniently sold
* Easily accessible
* Take anywhere/mobile
* Less chance of breakdown
* Can hold up to 256GB of data

**Online backups**

1. **Why do organisations use this form of backup?**

Organisations use this type of storage because it is of a low cost, is highly accessible and because it means that if the organisation’s equipment fails, the data is stored virtually and can be accessed anywhere.

1. **Describe an enterprise storage system.**

An enterprise storage system typically involves the interconnection via a storage area network, of RAID disks, tapes, CD/DVD ROM servers, internet backup and other networked storage devices.

**Surveillance technology, p 292**

**Describe the nature of the following items of surveillance equipment used in offices:**

1. **Packet sniffers**

Packet sniffers are diagnostic tools that monitor the contents of packets of data being sent across networks.

1. **Desktop monitoring programs**

Desktop monitoring programs work by intercepting every single action preformed on a computer. The monitoring program must be installed on the computer. Hackers also use Trojan horse programs to install this type of software.

1. **Log files**

Logs are kept of the applications run and currently being runand the users’ hat log onto the computer.

1. **Closed-circuit television, (CCTV)**

CCTV is a series of video cameras linked to an internal TV system. They are monitored and watched each day.

1. **Telephones**

Some employees are able to tap into the phone lines and listen to confidential conversations. Conversations can also be recorded and monitored.

1. **Audit trails**

An audit trail would include log files of system logins, both successful and unsuccessful, as well as any files that were accessed.

**Physical security devices:**

1. **List the options for physically securing your data**

* Lockable disk box
* Specialised room
* Safe
* Security cables
* Padlocks